UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,486	11/19/2003	Masahiro Fukui	60188-697	4493

7590 04/10/2007

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
GEBRESILASSIE, KIBROM K	
ART UNIT	PAPER NUMBER
2128	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/715,486	FUKUI ET AL.	
	Examiner	Art Unit	
	Kibrom K. Gebresilassie	2128	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is responsive to application filed on December 22, 2006.

2. Claims 1-17 are pending.

Response to Arguments

3. Response to Claim Objection: No response was presented for claims objected in pervious Office Action and therefore the objection is maintained.

4. Response to 103(a) rejection: Applicant's arguments filed December 22, 2006 have been fully considered but they are not persuasive.

a. Regarding Claim 1: Applicants argued that the prior art of reference does not disclose *intermediate data encryption means for encrypting intermediated data generated during simulation* and *intermediate data decrypting means for...providing ...decrypted intermediate data to the simulation means.*

Examiner respectfully disagrees. The prior art of reference (Bilchev et al) in view of Shiomi et al teaches the *intermediate data encryption means for encrypting intermediated data generated during simulation* (such as ***...a signal to be enciphered is input by the data input device....*; See: Col. 7 lines 65-66; and** ...***generates enciphered data...*; See: Col. 8 lines 47-50**) and *intermediate data decrypting means for...providing ...decrypted intermediate data to the simulation means* (such as ...***the deciphered data block then be output to the output device...*;See: Col. 8 lines 39-43)**. The prior art of reference (Bilchev et al) discloses the input and output device to input/output the enciphered and deciphered data's. However, Bilchev silent whether the input

device and/or output devices are a simulation means. Shiomi et al discloses a design/verification process (i.e. simulation means) (See: Shiomi et al, [0010]) that cures the deficiency of the prior art of Bilchev et al.

Applicants argued that the prior art of reference (Shiomi et al) would do reverse engineering for intermediate data encrypting means. Examiner respectfully disagrees. The prior art of reference (Shiomi et al) used only to show the design/verification process (i.e. simulation means), which is equivalent to the input/output device of the Bilchev et al.

b. Regarding Claims 2-3, 9, 11, 13, and 15: No argument were presented for these claims except they depend and/or recited the same limitation as Claim 4 and therefore the same argument will apply.

c. Regarding Claim 4: Applicant's arguments filed December 22, 2006 have been fully considered but they are not persuasive.

Applicants argued that the prior art of reference does not teach the encryption of previously decrypted data.

The prior art of reference (Bilchev et al) uses reversible cipher units (**See: Col. 5 lines 46-50**). In order to encrypt the signals it is passed from left to right, and in order to decrypt the signal it is passed from right to left of the cipher unit (**See: Col. 7 lines 12-16**).

Further, applicants argued that the prior art of reference does not disclose different encryption techniques. Examiner respectfully disagrees. The prior art of reference discloses different encryption techniques such as *using three-input*

logic gates, gates using multiplexers, and/or gates using three-state buses (**See: Col. 11 lines 25-47; Figs. 19-22**)

d. Regarding Claims 5-8, 10, 12, 14, 16, and 17: No argument were presented for these claims except they depend and/or recited the same limitation as Claim 4 and therefore the same argument will apply.

5. Therefore, the rejection of 103(a) is maintained.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,076,060 issued to Bilchev et al, in view of US Publication No. 2002/0083330 issued to Shiomi et al.

As per Claim 1:

Bilchev discloses a circuit operation simulating apparatus (**See: Col. 11 lines 48-51**) comprising:

storage means for storing encrypted circuit information (such as...***the encryption and storage of data in a computer to prevent unauthorized access...***; **See: Col. 3 lines 53-54**);

stored circuit information decrypting means for reading out the encrypted circuit information from the storage means (such as...***the storage of encrypted data for retrieval....***;**See: Col. 3 lines 59-60**), decrypting the circuit information, and providing the decrypted circuit information (such as ...***the deciphered data block can then be output to the output device...***; **See: Col. 8 lines 39-43**);

intermediate data encrypting means for encrypting intermediate data generated and storing the encrypted intermediate data in the storage means (such as ***...a signal to be enciphered is input by the data input device....***; **See: Col. 7 lines 65-66; and** ...***generates enciphered data...***; **See: Col. 8 lines 47-50**); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means, decrypting the intermediate data (such as ...***the enciphered data block has been deciphered...***; **See: 8 lines 35-40**), and providing the decrypted intermediate data (such as ...***the deciphered data block then be output to the output device...***;**See: Col. 8 lines 39-43**).

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev does not expressly teach the output device is simulation means for simulating operation

of a circuit based on circuit information on a configuration and characteristics of the circuit. Shiomi discloses simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit (such as...***design/verification process...***; **See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data. The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

As per Claim 2:

Shiomi discloses the circuit operation simulating apparatus of claim 1, wherein the stored circuit information decrypting means and the intermediate data decrypting means are combined together (such as ***...the circuit design data is encrypted together with the data of the expected value of the simulation result...***;**See: [0058] lines 1-3**).

As per Claim 3:

Shiomi discloses the circuit operation simulating apparatus of claim 1, including intermediate data deleting means for deleting the intermediate data stored in the

storage means, after the simulation has been terminated (**See: [0078]**).

As per Claim 4:

Bilchev discloses a circuit operation simulating apparatus (**See: Col. 11 lines 48-51**) comprising:

supplied circuit information decrypting means for decrypting supplied circuit information encrypted by a first encryption technique (such as ...***generates enciphered data...and then passed to another computer for deciphering...***; **See: col. 8 lines 47-50**);

stored circuit information encrypting means for encrypting, by a second encryption technique, the circuit information decrypted by the supplied circuit information decrypting means (**See: Col. 8 lines 24-35**);

storage means for storing the circuit information encrypted by the second encryption technique (such as...***generates enciphered data...this can be stored...***;**See: Col. 8 lines 46-48)**; and

stored circuit information decrypting means for reading out the circuit information encrypted by the second encryption technique from the storage means (such as...***the storage of encrypted data for retrieval....***;**See: Col. 3 lines 59-60**), decrypting the circuit information and providing the decrypted circuit information (such as ...***the deciphered data block can then be output to the output device...***; **See: Col. 8 lines 39-43**).

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev

does not expressly teach the output device is a simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit.

Shiomi discloses simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit (such as...***design/verification process...***; **See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data. The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

As per Claim 5:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the encryption by the first encryption technique has encryption strength higher than that by the second encryption technique (such as ...***the encryption between A and B in Fig. 19***).

As per Claim 6:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the encryption by the second encryption technique requires shorter time for encryption

and decryption than that by the first encryption technique (**See: *Fig. 20 and Fig. 21 encryption techniques which Fig. 21 takes short time for encryption and decryption than Fig. 20 because of the number of gates***).

As per Claim 7:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the circuit information decrypted by the supplied circuit information decrypting means is not stored in the storage means but encrypted by the stored circuit information encrypting means (**See: Fig. 15, Blocks S5, S6, and S7**).

As per Claim 8:

Bilchev discloses the circuit operation simulating apparatus of claim 4, including:

intermediate data encrypting means for encrypting intermediate data generated during a simulation by the simulation means and for storing the encrypted intermediate data in the storage means (such as...***formed into enciphered data blocks...the passage of enciphered data blocks into a working memory...***; **See: Col. 8 lines 26-29**); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means, decrypting the intermediate data (such as ...***the enciphered data block has been deciphered...***; **See: 8 lines 35-40**), and providing the decrypted intermediate data to the simulation means, (such as ...***the deciphered data block then be output to the output device...***;**See: Col. 8 lines 39-43**), wherein the stored circuit information encrypting means and the intermediate data encrypting

means are combined together.

As per Claims 9, and 11-14:

The limitations of claims 9, and 11-14 have already been discussed in the rejection of claims 1, and 4. The instant claims is/are functionally equivalent to the above rejected claims and is/are therefore rejected under the same rationale.

As per Claim 10:

Bilchev discloses a circuit operation simulating apparatus comprising:

storage means for storing encrypted circuit information (such as...***the encryption and storage of data in a computer to prevent unauthorized access...***; **See: Col. 3 lines 53-54**), wherein the circuit operation simulating apparatus is configured to be able to incorporate:

supplied circuit information decrypting means for decrypting supplied circuit information encrypted by a first encryption technique (such as ...***generates enciphered data...and then passed to another computer for deciphering...***; **See: col. 8 lines 47-50**);

stored circuit information encrypting means for encrypting, by a second encryption technique, the circuit information decrypted by the supplied circuit information decrypting means, and for storing the encrypted circuit information in the storage means (**See: Col. 8 lines 24-35**); and

stored circuit information decrypting means for decrypting the circuit information read out from the storage means and encrypted by the second encryption technique (such as ...***the enciphered data block has been deciphered...***; **See: 8 lines 35-40**), and for providing the decrypted circuit information (such as ...***the deciphered data block then be output to the output device...***;**See: Col. 8 lines 39-43**).

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev does not expressly teach the output device is a simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit.

Shiomi discloses simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit (such as...***design/verification process...***; **See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data. The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

As per Claim 15:

Bilchev discloses a circuit operation simulating system for simulating operation of a circuit based on supplied circuit information on a configuration and characteristics of the circuit, the system comprising:

encryption means for encrypting circuit information to be supplied (such as ***...generates enciphered data...and then passed to another computer...***; **See: col. 8 lines 47-50**);

transmission means for transmitting the encrypted circuit information via a network (such as...***generates enciphered data...can be broadcast or transmitted over a network...***; **See: Col. 8 lines 46-51**);

reception means for receiving the transmitted circuit information (such as...***for reception by computer...***; **See: Col. 8 lines 50-52**);

storage means for storing the received circuit information (such as...***generates enciphered data...this can be stored...***;**See: Col. 8 lines 46-48**);

stored circuit information decrypting means for reading out the encrypted circuit information from the storage means and (such as...***the storage of encrypted data for retrieval....***;**See: Col. 3 lines 59-60**), decrypting the circuit information ((such as ***...the deciphered data block then be output to the output device...***;**See: Col. 8 lines 39-43**);

intermediate data encrypting means for encrypting intermediate data generated during a simulation by the simulation means and storing the encrypted intermediate data in the storage means (such as...***formed into enciphered data blocks...the***

***passage of enciphered data blocks into a working memory...*; See: Col. 8 lines 26-29**); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means, decrypting the intermediate data (such as ...***the enciphered data block has been deciphered...*; See: 8 lines 35-40**), and providing the decrypted intermediate data to the simulating means (such as ...***the deciphered data block then be output to the output device...*;See: Col. 8 lines 39-43**).

receiving the decrypted circuit information from the stored circuit information decrypting means (**See: Fig. 10 Block 240 and Fig. 11 Block 340**);

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev does not expressly teach the output device is a simulation means for simulating operation of the circuit based on the received circuit information.

Shiomi discloses simulation means for simulating operation of the circuit based on the received circuit information (such as...***design/verification process...*; See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data. The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design

data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

As per Claim 16:

Bilchev discloses a circuit operation simulating system for simulating operation of a circuit based on supplied circuit information on a configuration and characteristics of the circuit, the system comprising:

first encryption means for encrypting circuit information to be supplied, by a first encryption technique (such as ...***generates enciphered data...and then passed to another computer...***; **See: col. 8 lines 47-50**);

transmission means for transmitting the encrypted circuit information via a network (such as...***generates enciphered data...can be broadcast or transmitted over a network...***; **See: Col. 8 lines 46-51**);

reception means for receiving the transmitted circuit information (such as...***for reception by computer ...***; **See: Col. 8 lines 50-52**);

first decrypting means for decrypting the received circuit information (such as...***for reception by computer for deciphering there ...***; **See: Col. 8 lines 50-52**);

second encryption means for encrypting, by a second encryption technique, the circuit information decrypted by the first decrypting means (such as ...***generates enciphered data...and then passed to another computer for deciphering there...***; **See: col. 8 lines 47-50**);

storage means for storing the circuit information encrypted by the second encryption technique (such as...***the storage of encrypted data for retrieval....*;See: Col. 3 lines 59-60**);

second decrypting means for reading out the circuit information encrypted by the second encryption technique from the storage means and for decrypting the circuit information (such as ...***the enciphered data block has been deciphered...*; See: 8 lines 35-40**).

receiving the decrypted circuit information from the second decrypting means (**See: Fig. 10 Block 240 and Fig. 11 Block 340**)..

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev does not expressly teach the output device is a simulation means for simulating operation of the circuit based on the received circuit information.

Shiomi discloses simulation means for simulating operation of a circuit based on circuit information on a configuration and characteristics of the circuit (such as...***design/verification process...*; See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data. The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design

data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

As per Claim 17:

Bilchev discloses a circuit operation simulating system for simulating operation of a circuit based on supplied circuit information on a configuration and characteristics of the circuit, the system comprising:

first encryption means for encrypting circuit information to be supplied, by a first encryption technique (such as ...***generates enciphered data...and then passed to another computer...***; **See: col. 8 lines 47-50**);

second encryption means for further encrypting, by a second encrypted technique, the circuit information encrypted by the first encryption technique (such as ***...to encrypt the signal it is passed from left to right through the cipher units...***; **See: Col. 7 lines 12-14**);

transmission means for transmitting the circuit information encrypted by the second encryption technique, via a network (such as...***generates enciphered data...can be broadcast or transmitted over a network...***; **See: Col. 8 lines 46-51**);

reception means for receiving the transmitted circuit information (such as...***for reception by computer...***; **See: Col. 8 lines 50-52**);

first decrypting means for decrypting the received circuit information encrypted by the second encryption technique (such as ...***generates enciphered data...and then passed to another computer for deciphering there...***; **See: col. 8 lines 47-50**) and for outputting the circuit information encrypted by the first encryption technique (such as

...***generates enciphered data...and then passed to another computer...***; **See: col. 8 lines 47-50**);

storage means for storing the circuit information output from the first decrypting means and encrypted by the first encryption technique (such as...***the storage of encrypted data for retrieval....***;**See: Col. 3 lines 59-60**);

second decrypting means for reading out the circuit information encrypted by the first encryption technique from the storage means and for decrypting the circuit information (such as...***the storage of encrypted data for retrieval....***;**See: Col. 3 lines 59-60**); and

simulation means for receiving the decrypted circuit information from the second decrypting means (such as ...***the deciphered data block then be output to the output device...***;**See: Col. 8 lines 39-43**).

Bilchev discloses outputting the enciphered data and deciphered data block to the output device (**See: Fig. 10 Block 240 and Fig. 11 Block 340**). However, Bilchev does not expressly teaches the output device is simulation means for simulating operation of the circuit based on the received circuit information.

Shiomi discloses simulation means for simulating operation of the circuit based on the received circuit information (such as...***design/verification process...***; **See: [0058]**).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Shiomi et al with Bilchev et al because both references are clearly concerned with encryption and/or decryption of design data.

The motivation for doing so would have been convenient to connect simulation means (i.e. design/verification process) for simulating operation of a circuit, as taught by Shiomi et al, for encipher units of Bilchev et al to verify the circuit operation for the circuit design data and further to compare the actual output value with the expected value (**See: Shiomi et al, [0010]**).

Conclusion

8. Claims 1-17 are rejected.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Communication

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kibrom K. Gebresilassie whose telephone number is 571-272-8571. The examiner can normally be reached on 8:00 am - 4:30 pm Monday to Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner supervisor, Kamini Shah can be reached at (571) 272-2279. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kibrom Gebresilassie
AU 2128

KAMINI SHAH
SUPERVISORY PATENT EXAMINER